

申請日期	89 年 3 月 10 日
案 號	89104427
類 別	G06F 15/00 12/00

(以上各欄由本局填註)

A4  
C4

公告本

470889

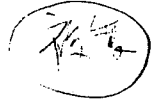
發 明 專 利 說 明 書		
一、發明 新型名稱	中 文	電腦系統及內容保護方法
	英 文	
二、發明 創作人	姓 名	(1) 石橋泰博 (2) 上林達 (3) 田村正文
	國 籍	(1) 日本                      (2) 日本                      (3) 日本 (1) 日本國東京都青梅市新町九一四一一 魯美耶 魯新町一一三一三
	住、居所	(2) 日本國神奈川縣茅ヶ崎市本宿町三一一八一一 〇八 (3) 日本國東京都調布市調布ヶ丘一一一八七六 一七〇六
三、申請人	姓 名 (名稱)	(1) 東芝股份有限公司 株式会社東芝
	國 籍	(1) 日本
	住、居所 (事務所)	(1) 日本國神奈川縣川崎市幸區堀川町七二番地
	代 表 人 姓 名	(1) 西室泰三

本紙張尺度適用中國國家標準 (CNS) A4規格 (210×297公釐)

## 四、中文發明摘要(發明之名稱：

## 電腦系統及內容保護方法

本發明係關於電腦系統及被適用於該電腦系統之內容保護方法。其手段為：安全管理者(112)在使用具有媒體ID之記錄媒體(116、117)之情形，於每個記錄內容之記錄媒體使用該媒體ID進行內容之加密/解碼之管理。另一方面，在使用不具有媒體ID之HDD(115)之情形，安全管理者(112)透過BIOS取得電腦系統之固有的裝置ID，使用該裝置ID管理記錄在HDD之內容之加密/解碼。裝置ID被記憶在電腦系統內之安全的領域。藉由此，即使在硬碟之類的開放式記錄媒體中記錄內容之情形，可以保護該內容被不正當使用，能一併謀求數位內容之利用與保護。



## 英文發明摘要(發明之名稱：

(由本局填寫)

承辦人代碼：
大 類：
I P C 分類：

A6  
B6

本案已向：

國(地區) 申請專利，申請日期：

案號：

，☐有 ☐無主張優先權

日本

1999 年 4 月 28 日 11-122001

☒有主張優先權

有關微生物已寄存於：

，寄存日期：

，寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

經濟部智慧財產局員工消費合作社印製

## 五、發明說明( 1 )

### 發明背景

本發明係關於電腦系統及被適用於該電腦系統之內容保護方法。

近年來伴隨電腦技術之發達，各式各樣之對應多媒體之個人電腦正被開發著。此種個人電腦可以通過網路下載影像資料或音樂資料等之數位內容使用。

這些數位內容藉由MPEG2、MP3之所謂的數位編碼技術之採用，可以不降低品質下載。因此，最近由著作權保護之觀點而言，保護此種數位內容被不正當使用之技術必要性乃隨之產生。

但是，個人電腦基本上為具有開放構造之系統之故，個人電腦之數位內容之保護實際上有其困難。此係由於在個人電腦上雖然數位內容係以檔案形式被處理，但是檔案之複製／移動基板上可以自由進行之故也。特別是關於被當成個人電腦之儲存裝置使用之硬碟機，其之規格係開放式，謀求被記錄於硬碟機上之數位內容之祕密化很困難。因此，由網際網路下載之數位內容一旦記錄在硬碟機後，可以將該數位內容由硬碟機自由地複製於其它之媒體使用。

### 發明摘要

因此，本發明之目的在於提供：即使在硬碟機之類的開放式記憶媒體中記錄內容之情形，可以保護該內容被不正當使用，能一併謀求數位內容之利用與保護之電腦系統。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明( 2 )

及內容保護方法。

依據本發明之一觀點，提供一種在記錄媒體可以記錄內容之電腦系統，其特徵係包含：爲了應記錄於前述記錄媒體之內容管理，記憶對應前述記憶媒體之 I D 之 I D 記憶手段，該 I D 記憶手段係有別於前述記錄媒體而設置；及在前述記錄媒體記錄內容之時，藉由前述 I D 記憶手段使用對應前述記憶媒體之 I D，實施記錄前述內容之加密之內容管理手段。

依據本發明之其它觀點，提供一種在記錄媒體可以記錄內容之電腦系統，其特徵係包含：記憶限制被附加在前述內容之再生／複製／移動用之控制資訊，以及對應前述記錄媒體之 I D 之記憶手段，該 I D 記憶手段係有別於前述記錄媒體而設置；及在被記錄於前述記錄媒體之內容的再生、或對其它記錄媒體之複製或移動被要求時，依據前述控制資訊與前述 I D，許可或禁止前述被要求之處理的實行之內容管理手段。

依據本發明之其它的觀點，係提供一種電腦系統，其特徵係包含：記憶被使用於內容之安全管理用之裝置 I D 之裝置 I D 記憶手段；及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之裝置 I D，可以管理前述內容之加密／解碼之內容管理手段，在不具有前述裝置 I D 之記錄媒體記錄內容之情形，使用前述裝置 I D 管理前述內容之加密／解碼之內容管理手段。

依據本發明之其它觀點，係提供一種電腦系統，其特

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

### 五、發明說明 ( 3 )

徵係包含：記憶被使用於內容之安全管理用之裝置 I D 之裝置 I D 記憶手段；及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之媒體 I D，可以管理前述內容之加密／解碼之內容管理手段，在不具有前述媒體 I D 之記錄媒體記錄內容之情形，使用前述裝置 I D 管理前述內容之加密／解碼之內容管理手段，其中前述裝置 I D 記憶手段之裝置 I D 係藉由前述電腦系統之 B I O S 被管理，前述內容管理手段藉由與前述 B I O S 之認證由前述 B I O S 取得前述裝置 I D，在前述內容被附加限制該內容之再生／複製／移動用之限制資訊，前述 B I O S 管理前述控制資訊之改變檢測用之編碼資料，前述內容管理手段在將被記錄於不具有前述媒體 I D 之內容複製於其它記錄媒體之情形，使前述內容之複製可能次數減少 1 地更新不具有前述媒體 I D 之記錄媒體內之控制資訊，同時將被記錄於不具有前述媒體 I D 之記錄媒體之內容與前述更新後之控制資訊複製於前述其它之記錄媒體，而且依據更新後之控制資訊更新前述改變檢測用編碼資料之值。

依據本發明之進一步之其它的觀點，係提供一種可以處理內容之電腦系統，其特徵為包含：進行前述內容之安全管理之內容管理手段，該內容管理手段包含：在具有媒體 I D 之記錄媒體記錄內容之情形，使用前述媒體 I D 加密前述內容或該內容之密碼鍵，記錄於具有前述媒體 I D 之記錄媒體之手段；及在不具有媒體 I D 之記錄媒體記錄內容之情形，使用藉由前述電腦系統之 B I O S 被管理之

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明( 4 )

前述電腦系統固有之裝置 I D，加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體 I D 之記錄媒體之手段。

依據本發明之其它的觀點，係提供一種電腦系統，其特徵為包含：電腦系統之硬體控制用之系統程式，該系統程式管理前述電腦系統固有之裝置 I D；及利用前述電腦系統固有之裝置 I D，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼之內容管理手段。

依據本發明之其它的觀點，係提供一種在電腦系統具有固有之裝置 I D 之電腦系統，其特徵為包含：由前述電腦系統取得前述裝置 I D，使用該取得之裝置 I D，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼之內容管理手段。

依據本發明之其它的觀點，係提供一種被適用於可以處理內容之電腦系統，保護前述內容被不正當使用之內容保護方法，其特徵為：在具有媒體 I D 之記錄媒體記錄內容之情形，使用前述媒體 D 加密前述內容或該內容之密碼鍵，記錄於具有前述媒體 I D 之記錄媒體；及在不具有媒體 I D 之記錄媒體記錄內容之情形，使用藉由前述電腦系統內之 B I O S 被管理之前述電腦系統固有之裝置 I D，加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體 I D 之記錄媒體。

依據本發明之其它的觀點，係提供一種保護以具有系統固有之裝置 I D 之電腦系統被處理之內容被不正當使用之內容保護方法，其特徵為：由前述電腦系統取得前述裝

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明( 5 )

置 I D ; 及使用前述取得之裝置 I D , 管理應記錄於前述電腦系統之記錄媒體之內容之加密 / 解碼。

依據本發明之其它的觀點, 係提供一種保護在電腦系統被處理之內容被不正當使用之內容保護方法, 其特徵為: 藉由前述電腦系統之硬體控制用之系統程式管理前述電腦系統固有之裝置 I D , 由前述系統程式取得前述裝置 I D ; 及使用前述取得之裝置 I D , 管理應記錄於前述電腦系統之記錄媒體之內容之加密 / 解碼。

### 發明之詳細說明

以下, 參考圖面說明本發明之實施形態。

圖 1 係顯示本發明之一實施形態之個人電腦之系統構成。此個人電腦 ( P C ) 1 1 為可以處理影像資料或音樂資料等之各種數位內容之電腦系統。此個人電腦 1 1 之內容保護方法係以: 在每個應記錄內容之媒體利用該記錄媒體之媒體 I D 以管理內容之加密 / 解碼為前提。此係如為同一記錄媒體, 為了使之在其它個人電腦或電子機器使用也可以再生該記錄媒體之故, 內容係使用被準備在各記錄媒體之專用的媒體 I D 以加密被記錄著。使用媒體 I D 之內容的加密 / 解碼之管理係藉由為此之專用的軟體之安全管理者 1 1 2 被實行。此安全管理者 1 1 2 係以篡改 . 防止 . 軟體而被實現。所謂篡改 . 防止 . 軟體係意指: 對於不正當之內部解析或篡改等之攻擊 ( attack ) 具備防衛機能之軟體。



## 五、發明說明 ( 6 )

安全管理者 1 1 2 係如圖示般地，位於應用程式 1 1 1 與檔案系統 1 1 3 之間，保護對向之內容之「記錄」、「再生」、「複製」、「移動」等之各種操作係透過安全管理者 1 1 2 進行。藉由安全管理者 1 1 2 之內容的加密／解碼管理可以大致區分為：1) 對於內藏專用之媒體 I D 之記錄媒體者，及 2) 對於不具有媒體 I D 之通常的記錄媒體者。

( 具有媒體 I D 之記錄媒體 )

首先，說明對於具有媒體 I D 之記錄媒體之處理。

記錄媒體 ( A ) 1 1 6 以及記錄媒體 ( B ) 1 1 7 係分別對應安全管理者 1 1 2 之專用記錄媒體。這些記錄媒體可以使用可以安裝、拆下自如地裝置在個人電腦 1 1 或其它之各種電子機器之記憶卡等之各種媒體 ( S S F D C 、快閃 P C 卡、迷你碟 ) 等。

在記錄媒體 ( A ) 1 1 6 在通常之資料記憶領域之外，設置有：該記錄媒體固有之媒體 I D ( I D A ) 被預先記憶之 R O M 領域，以及儲存由後述之 G I ( Governance Information : 管理資訊 ) 表所製作之 G I 校驗和資料用之 G I 校驗和領域。記錄媒體 ( B ) 1 1 7 也係同樣構成。媒體 I D 只要是各記錄媒體所固有即可，可以使用序列號碼或製造號碼、其它各樣之辨識資訊。

所謂 G I 表係對每一保護對象之各內容規定其之再生、複製、移動之可否、以及複數可能次數、移動可能次數

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 7 )

等之複製控制資訊。G I 校驗和資料係檢測 G I 表之內容之篡改用之改變檢測用編碼資料，由 G I 表之值被計算出。也可以使用 G I 表之雜碼 ( hash ) 值以代替 G I 校驗和資料。G I 表之「複製可能次數」之值在複製每被實行時被減掉 1。如此在 G I 表之值被更新之時，配合該更新，G I 校驗和資料之值也被更新。因此，G I 校驗和領域係由可以重寫之領域構成。

R O M 領域以及 G I 校驗和領域之任一種皆係使用者無法存取之安全領域。

在將內容記憶於記錄媒體 ( A ) 1 1 6 之情形，安全管理者 1 1 2 使用記錄媒體 ( A ) 1 1 6 之媒體 I D 管理內容之加密／解碼。在此情形，以下之資料被儲存在記錄媒體 ( A ) 1 1 6 之資料領域。

- ． K c [ Content ] : 藉由被稱為內容 K c 之密碼鍵 被加密之內容
- ． G I
- ． I D A [ K c ] : 藉由記錄媒體 ( A ) 1 1 6 之媒體 I D ( I D A ) 被加密之內容鍵

在再生被記錄於記錄媒體 ( A ) 1 1 6 之內容之情形，安全管理者 1 1 2 首先使用記錄媒體 ( A ) 1 1 6 之媒體 I D ( I D A )，解碼 I D A [ K c ]，獲得 K c。而且，藉由該 K c 解碼 K c [ Content ]。

被記錄於記錄媒體 ( A ) 1 1 6 之內容如為可以複製之內容之情形，可以將該內容由記錄媒體 ( A ) 1 1 6 複

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 8 )

製於其它之記錄媒體 ( 例如記錄媒體 ( B ) 1 1 7 ) 。在此情形，安全管理者 1 1 2 由被儲存在記錄媒體 ( A )

1 1 6 之 G I 產生校驗和，將該校驗和資料與記錄媒體 ( A ) 1 1 6 之 G I 校驗和領域之 G I 校驗和資料比較。在不一致之情形，複製被禁止。在一致之情形，安全管理者 1 1 2 使用記錄媒體 ( A ) 1 1 6 之媒體 I D ( I D A ) 解碼 I D A [ K c ]，獲得 K c。接著，安全管理者

1 1 2 使用複製目的地之記錄媒體 ( B ) 1 1 7 之媒體 I D ( I D B )，加密 K c，將加密之內容鍵 ( I D B [ K c ] ) 與 K c [ Content ] 以及 G I 一齊地寫入記錄媒體 ( B ) 1 1 7 之資料領域。在此情形，記錄媒體 ( A )

1 1 6、記錄媒體 ( B ) 1 1 7 之藉由 G I 被指定之可以複製次數之值都被減少 1。例如，在複製之內容為「只可複製一次」之內容之情形，被變更為「無法再複製」之內容。又，伴隨 G I 之更新，記錄媒體 ( A ) 1 1 6、記錄媒體 ( B ) 1 1 7 之各別的 G I 校驗和之值也被更新。

被記錄於記錄媒體 ( A ) 1 1 6 之內容為可以移動之內容之情形，可以將該內容由記錄媒體 ( A ) 1 1 6 移動於其它之記錄媒體 ( 記錄媒體 ( B ) 1 1 7 )。在此情形，安全管理者 1 1 2 由被儲存於記錄媒體 ( A ) 1 1 6 之 G I 產生校驗和資料，將該校驗和資料與記錄媒體 ( A ) 1 1 6 之 G I 校驗和領域之 G I 校驗和資料比較。在不一致之情形，移動被禁止。在一致之情形，安全管理者

1 1 2 使用記錄媒體 ( A ) 1 1 6 之媒體 I D ( I D A )

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 9 )

，解碼 I D A [ K c ] ，獲得 K c 。接著，安全管理者 1 1 2 使用移動目的地之記錄媒體 ( B ) 1 1 7 之媒體 I D ( I D B ) ，加密 K c ，將加密之內容鍵 ( I D B [ K c ] ) 與 K c [ Content ] 以及 G I 一齊地寫入記錄媒體 ( B ) 1 1 7 之資料領域。之後，安全管理者 1 1 2 消除被儲存在移動源之記錄媒體 ( A ) 1 1 6 之資料領域之 K c [ Content ] 、 G I 、 I D A [ K c ] ，同時消除 G I 校驗和領域之 G I 校驗和資料。在藉由 G I 被規定者在只是「複製可能次數」而未規定「移動可能次數」之情形，不進行因移動之 G I 的更新。在「移動可能次數」被規定之情形，與前述之「複數」之情形相同，在 G I 被更新後，被寫入記錄媒體 ( B ) 1 1 7 ，又，對應該更新後之 G I 之校驗和資料變成被寫入 G I 校驗和領域。

( 不具有媒體 I D 之記錄媒體 )

接著，說明對於不具有媒體 I D 之處理。

H D D 1 1 5 係被當成個人電腦 1 1 之二次記憶裝置使用之儲存裝置，被固定於個人電腦 1 1 而使用。在

H D D 1 1 5 並沒有設置記錄媒體 ( A ) 1 1 6 以及記錄媒體 ( B ) 1 1 7 之類的 R O M 領域或 G I 校驗和領域。

使用 H D D 1 1 5 進行內容之記錄、複製、移動等之情形，安全管理者 1 1 2 使用本個人電腦 1 1 所固有之裝置 I D 以代替媒體 I D，進行內容之加密／解碼之管理。即安全管理者 1 1 2 在內容之記錄目的地、複製目的地、

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 10 )

複製源、移動目的地或移動源為對應 H D D 1 1 5 之驅動器號碼之情形，並非使用媒體 I D 而係使用在系統內被管理之裝置 I D。在此情形，哪個驅動器號碼之記錄媒體具有媒體 I D，哪個驅動器號碼之記錄媒體不具有媒體 I D 例如藉由利用隨插即用等之機能，可以使安全管理者 1 1 2 可以每個媒體都能辨識。

P C 1 1 固有之裝置 I D 係藉由 P C 1 1 之硬體控制用之系統程式之 B I O S 被管理。在此 B I O S 之管理下，設置有：快閃 B I O S - R O M 1 4、鑲嵌式控制器（副 C P U）1 2 1 以及快閃 R O M 1 2 2。

快閃 B I O S - R O M 1 1 4 具有使用者無法存取之安全領域，在此如圖 2 所示般地，除了通行密碼區域之外，設置有 I D 區域、校驗和區域。通行密碼區域為記憶依據使用者被登錄之通行密碼用之領域。在通行密碼被登錄之情形，判斷電源投入時由使用者輸入之通行密碼與登錄通行密碼之一致的有無，只在一致之情形，由 O S 之保護或暫停／睡眠狀態之回復變成可能。

P C 1 1 固有之裝置 I D ( I D S ) 被預先記憶在 I D 區域。校驗和區域係被使用於由被記憶在 H D D 1 1 5 之內容的 G I 產生 G I 校驗和資料之儲存。

另一方面，鑲嵌式控制器 1 2 1 相當於鍵盤控制器或電源控制器，在 B I O S 之控制下，可以存取快閃 R O M 1 2 2。快閃 R O M 1 2 2 具有與快閃 B I O S - R O M 1 1 4 同樣之安全領域。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 11 )

上述 I D S 以及 G I 校驗和資料雖然被儲存在快閃 B I O S - R O M 1 1 4 與快閃 R O M 1 2 2 之中之任何一個的安全領域都可以，但是在本實施形態中，以利用快閃 B I O S - R O M 1 1 4 之安全領域為例說明之。

在 B I O S 設置與安全管理者 1 1 2 之間進行認證處理用之認證機能。藉由安全管理者 1 1 2 與 B I O S 之認證處理一被確認互相彼此為正確的程式，安全管理者 1 1 2 可以由 B I O S 取得裝置 I D ( I D S )。如此，藉由與 B I O S 之認證第 1 次取得裝置 I D，可以更安全地管理裝置 I D。

接著，參考圖 3 以及圖 5 具體說明使用 H D D 1 1 5 之情形之內容管理處理之順序。

### 「記錄」

圖 3 係顯示內容記錄時之動作流程。

(步驟 S 1)：在 P C 1 1 之啟動時，首先在安全管理者 1 1 2 與 B I O S 之間實行認證處理。一被確認彼此為互相正確之程式，在安全管理者 1 1 2 與 B I O S 之間進行鍵交換，同一之認證鍵 ( K x 2 ) 被共有。認證鍵 ( K x 2 ) 係每次改變之時變鍵。

(步驟 S 2)：安全管理者 1 1 2 對 B I O S 發行 I D 取得要求。響應由安全管理者 1 1 2 之 I D 取得要求，B I O S 將裝置 I D ( I D S ) 以認證鍵 ( K x 2 ) 加密，將被加密之裝置 I D ( K x 2 [ I D S ] ) 發送於安

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 12 )

全管理者 1 1 2。安全管理者 1 1 2 保持認證鍵 (  $K \times 2$  ) 之故，可以由  $K \times 2 [IDS]$  解讀  $IDS$ 。

(步驟 S 3)：在使用 WEB 瀏覽器等之應用程式由 WEB 伺服器下載影像資料或音樂資料等之內容之情形，透過 WEB 瀏覽器或直接在安全管理者 1 1 2 與 WEB 伺服器 1 2 間進行認證處理。一被確認為彼此互相具有正確內容保護機能者，在安全管理者 1 1 2 與 WEB 伺服器 1 2 之間進行鍵交換，同一之認證鍵 (  $K \times 1$  ) 被共有。認證鍵 (  $K \times 1$  ) 係每次改變之時變鍵。

(步驟 S 4)：WEB 伺服器 1 2 將被要求之內容以規定之內容鍵  $K_c$  加密之 (  $K_c [Content]$  ) 以及以認證鍵 (  $K \times 1$  ) 加密之內容鍵 (  $K \times 1 [K_c]$  ) 以及 GI 發送於 PC 1 1。

(步驟 S 5)：這些  $K_c [Content]$ 、 $K \times 1 [K_c]$ 、GI 透過 WEB 瀏覽器等被送往安全管理者 1 1 2。安全管理者 1 1 2 在由 WEB 瀏覽器指定之下載目的地之記錄媒體為 HDD 1 1 5 之情形，使用認證鍵 (  $K \times 1$  ) 與由 BIOS 取得之裝置 ID (  $IDS$  )，將  $K \times 1 [K_c]$  轉換為  $IDS [K_c]$ 。在此情形，首先，使用認證鍵 (  $K \times 1$  )， $K \times 1 [K_c]$  被解碼為  $K_c$ ，該  $K_c$  重新藉由  $IDS$  被加密。

之後，安全管理者 1 1 2 將  $K_c [Content]$ 、 $IDS [K_c]$ 、GI 通過檔案系統 1 1 3，進而 IDE 驅動器等，寫入 HDD 1 1 5。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 13 )

( 步驟 S 6 ) : 安全管理者 1 1 2 由 G I 算出 G I 校驗和資料 ( G I \_ C S ) , 將其以與 B I O S 之認證鍵 ( K x 2 ) 加密, 傳達於 B I O S 。 B I O S 將 G I 校驗和資料於被加密下或解碼後, 寫入快閃 B I O S - R O M 1 1 4 之校驗和區域。當然安全管理者 1 1 2 將 G I 校驗和資料或其之加密資料直接寫入快閃 B I O S - R O M 1 1 4 之校驗和區域也可以。

「再生」

圖 4 係顯示內容再生時之動作流程。

( 步驟 T 1 ) : 在 P C 1 1 之啟動時, 首先在安全管理者 1 1 2 與 B I O S 之間實行認證處理。一被確認彼此互相為正確程式, 在安全管理者 1 1 2 與 B I O S 之間進行鍵交換處理, 同一之認證鍵 ( 此處設為 K x 1 ) 被共有。認證鍵 ( K x 1 ) 為每次改變之時變鍵。

( 步驟 T 2 ) : 響應由安全管理者 1 1 2 之 I D 取得要求, B I O S 將裝置 I D ( I D S ) 以認證鍵 ( K x 2 ) 加密, 將被加密之裝置 I D ( K x 1 [ I D S ] ) 發送於安全管理者 1 1 2 。安全管理者 1 1 2 保持認證鍵 ( K x 1 ) 之故, 可以由 K x 1 [ I D S ] 解讀 I D S 。

( 步驟 T 3 ) : 接著, 響應安全管理者 1 1 2 來之 G I 校驗和資料之取得要求, B I O S 以認證鍵 ( K x 1 ) 加密 G I 校驗和資料 ( G I \_ C S ) , 將被加密之 G I 校驗和資料 ( K x 1 [ G I \_ C S ] ) 發送於安全管理者

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線



## 五、發明說明 ( 14 )

1 1 2。安全管理者 1 1 2 保持認證鍵 ( K x 1 ) 之故，可以由 K x 1 [ G I - C S ] 解讀 G I - C S。

( 步驟 T 4 )：安全管理者 1 1 2 透過檔案系統

1 1 3，進而 I D E 驅動器等由 H D D 1 1 5 取得由應用程式 1 1 1 等被指定之再生對象之被加密之內容 ( ( K c [ Content ] ) ) 以及與其對應之 I D S [ K c ] 以及 G I。

( 步驟 T 5 )：安全管理者 1 1 2 由 G I 算出校驗和，將該算出之校驗和與由 B I O S 取得之 G I - C S 比較。在不一致之情形，有 H D D 1 1 5 之 G I 藉由具惡意之使用者被重寫之虞之故，再生處理在此時終止。在一致之情形，安全管理者 1 1 2 使用由 B I O S 取得之 I D S，解碼 I D S [ K c ]，獲得 K c。而且使用該 K c 解除 K c [ Content ] 之密碼，將未加工之內容 ( Content ) 送往再生軟體 ( 再生裝置 )。再生軟體也以篡改、防止、軟體而被實現。

「複製」

圖 5 係顯示內容複製時之動作流程。此處例示將被記錄於 H D D 1 1 5 之內容複製於記錄媒體 ( A ) 1 1 6 之情形。

( 步驟 U 1 )：在 P C 1 1 之啟動時，首先在安全管理者 1 1 2 與 B I O S 之間實行認證處理。一被確認彼此互相為正確程式，在安全管理者 1 1 2 與 B I O S 之間進

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 15 )

行鍵交換處理，同一之認證鍵（此處設為  $K \times 1$ ）被共有。  
認證鍵（ $K \times 1$ ）為每次改變之時變鍵。

（步驟 U 2）：響應由安全管理者 1 1 2 之 ID 取得要求，BIOS 將裝置 ID（IDS）以認證鍵（ $K \times 2$ ）加密，將被加密之裝置 ID（ $K \times 1 \{ IDS \}$ ）發送於安全管理者 1 1 2。安全管理者 1 1 2 保持認證鍵（ $K \times 1$ ）之故，可以由  $K \times 1 \{ IDS \}$  解讀 IDS。

（步驟 U 3）：接著，響應安全管理者 1 1 2 來之 GI 校驗和資料之取得要求，BIOS 以認證鍵（ $K \times 1$ ）加密 GI 校驗和資料（GI - CS），將被加密之 GI 校驗和資料（ $K \times 1 \{ GI - CS \}$ ）發送於安全管理者 1 1 2。安全管理者 1 1 2 保持認證鍵（ $K \times 1$ ）之故，可以由  $K \times 1 \{ GI - CS \}$  解讀 GI - CS。

（步驟 U 4）：安全管理者 1 1 2 透過檔案系統 1 1 3，進而 IDE 驅動器等由 HDD 1 1 5 取得由應用程式 1 1 1 等被指定之複製對象之被加密之內容（（ $K \times 1 \{ Content \}$ ））以及與其對應之 IDS（ $K \times 1$ ）以及 GI。

安全管理者 1 1 2 由 GI 算出校驗和，將該算出之校驗和與由 BIOS 取得之 GI - CS 比較。在不一致之情形，有 HDD 1 1 5 之 GI 藉由具惡意之使用者被重寫之虞之故，複製處理在此時終止。在一致之情形，參考 HDD 1 1 5 之 GI，調查複製對象之內容是否為可以複製之內容。在「不可複製」或「複製可能次數 = 零」之情

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

## 五、發明說明 ( 16 )

形，複製處理在此時終止。如係可被複製之內容，安全管理者 1 1 2 進入下述之步驟 U 5 以後之處理。

( 步驟 U 5 ) : 安全管理者 1 1 2 進行與複製目的地之記錄媒體 ( A ) 1 1 6 或控制其之裝置驅動器之間之認證處理。一被確認彼此互相具有正確內容保護機能，在安全管理者 1 1 2 與複製目的地之記錄媒體 ( A ) 1 1 6 或其之裝置驅動器之間進行鍵交換，同一之認證鍵 ( 此處設為  $K \times 2$  ) 被共有。認證鍵 (  $K \times 2$  ) 為每次改變之時變鍵。

( 步驟 U 6 ) : 響應由安全管理者 1 1 2 之 I D 取得要求，記錄媒體 ( A ) 1 1 6 或其之裝置驅動器以認證鍵 (  $K \times 2$  ) 加密媒體 I D ( I D A ) ，將被加密之媒體 I D (  $K \times 2$  [ I D A ] ) 發送於安全管理者 1 1 2 。安全管理者 1 1 2 保持認證鍵 (  $K \times 2$  ) 之故，可以由  $K \times 2$  [ I D A ] 解讀 I D A 。

( 步驟 U 7 ) : 安全管理者 1 1 2 更新由 H D D 1 1 5 取得之 G I ，獲得「複製可能次數」被減 1 之  $G I'$  。而且，使用由 B I O S 取得之裝置 I D ( I D S ) ，解碼 I D S [  $K_c$  ] ，獲得  $K_c$  。接著，安全管理者 1 1 2 使用媒體 I D A 加密  $K_c$  ，獲得 I D A [  $K_c$  ] 。之後，安全管理者 1 1 2 將  $K_c$  [ Content ] 、 I D A [  $K_c$  ] 、  $G I'$  透過檔案系統 1 1 3 進而記錄媒體 ( A ) 1 1 6 之驅動器等寫入記錄媒體 ( A ) 1 1 6 。

( 步驟 U 8 ) : 安全管理者 1 1 2 算出由  $G I'$  之校

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 17 )

驗和資料 ( G I ' \_ C S ) , 將其以認證鍵 ( K x 2 ) 加密者 ( K x 2 [ G I ' \_ C S ] ) 發送於記錄媒體 ( A ) 1 1 6 或其之驅動器, 將 G I ' \_ C S 寫入記錄媒體 ( A ) 1 1 6 之 G I 校驗和資料領域。

( 步驟 U 9 ) : 之後, 安全管理者 1 1 2 將校驗和資料 ( G I ' \_ C S ) , 以與 B I O S 之認證鍵 ( K x 1 ) 加密, 將其傳達於 B I O S 。 B I O S 將快閃 B I O S - R O M 1 1 4 之校驗和區域之內容重寫於 G I ' \_ C S 。

( 步驟 U 1 0 ) : 而且, 安全管理者 1 1 2 將 H D D 1 1 5 之 G I 更新為 G I ' 。

### 「移動」

在將被記錄於 H D D 1 1 5 之內容移動於記錄媒體 ( A ) 1 1 6 之情形, 與圖 5 之複製處理基本上雖係以相同順序進行, 但是與複製處理不同之點為: 取代步驟 U 9 , 進行消除快閃 B I O S - R O M 1 1 4 之校驗和區域之內容之處理, 又, 取代圖 5 之步驟 U 1 0 , 進行消除 H D D 1 1 5 之 K c [ Content ] 、 I D S [ K c ] 、以及 G I 之處理。又, 移動之情形, 不進行對於複製可能次數之 G I 的更新, 除了移動可能次數被規定之情形, G I 不被更新地被寫入移動目的地之記錄媒體 ( A ) 1 1 6 。

如上述般地, 本實施形態中, 藉由使 B I O S 具有與安全管理者 1 1 2 之認證機能或裝置 I D 管理機能, 即使在不具有裝置 I D 之記錄媒體記錄內容之情形, 與使用具

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 18 )

有媒體 I D 之專用的記錄媒體之情形相同地，可以謀求被記錄於其上之內容之保護。

特別是藉由 B I O S 管理裝置 I D 以及 G I 校驗和資料，使無法由系統側存取之故，對於 H D D 1 1 5 不用加上任何變更，可以保護下載於 H D D 1 1 5 之內容被不正當使用。

又，在本實施形態中，雖然使用媒體 I D 或裝置 I D 加密內容之密碼鍵之內容鍵，但是也可以將媒體 I D 或裝置 I D 當成內容鍵使用，使用媒體 I D 或裝置 I D 加密內容本身。

又，在本實施形態中，雖然以 H D D 為不具有媒體 I D 之記憶媒體為例，但是使用裝置 I D 以進行加密／解碼之管理之本實施形態之內容保護方法例如對於 M O 或記憶卡（ P C 卡獲緻密快閃記憶卡等）或智慧媒體等不具有媒體 I D 之通常的不揮發性記憶媒體全體都可以適用。

又，裝置 I D 可以記憶於 P C 1 1 內之安全的記憶裝置，例如也可以記憶於 P C 1 1 內之埋入控制器（ E C ）內，被設置在 P C 1 1 內之即時時脈內之以電池備援之 C M O S 之記憶體等。即使在 P C 1 1 內之任何地方記憶裝置 I D 之情形，藉由透過 B I O S 取得裝置 I D，安全管理者 1 1 2 可以不意識裝置 I D 之記憶場所進行必要之處理。

再者，本實施形態不限於 P C，也可以適用於機上盒（ setup box ）、遊戲機、音頻／錄像機等、搭載微處理器

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

## 五、發明說明 ( 19 )

之所有的資料處理裝置 ( 電腦應用機器 ) 。

又，安全管理者 1 1 2 之機能，即藉由將包含：如前述般地由 B I O S 取得裝置 I D，使用該裝置 I D 管理內容之加密／解碼之順序，或具有媒體 I D 之記錄媒體使用該媒體 I D 管理內容之加密／解碼之順序等之電腦程式透過通訊媒體或記錄媒體導入電腦，藉由 B I O S 可以管理裝置 I D 之系統，可以獲得與本實施形態相同之效果。

又，B I O S 也是可以更新之故，在通常之硬體控制機能之外，如將具有裝置 I D 以及其之管理機能等之新的 B I O S 透過通訊媒體或記錄媒體導入電腦，即使在既存之電腦也可以獲得與本實施形態相同之效果。

如以上詳細敘述般地，依據本發明，即使在硬碟機之類的開放式記錄媒體記錄內容之情形，可以保護該內容被不正當使用，可以一併謀求數位內容之利用與保護。

### 圖面之簡單說明

圖 1 係顯示本發明之一實施形態之電腦系統之基本構成方塊圖。

圖 2 係顯示被設於同一實施形態之電腦系統之快閃 B I O S \_ R O M 之記憶內容之一例圖。

圖 3 係顯示在同一實施形態之電腦系統所進行之內容記錄處理之順序圖。

圖 4 係顯示在同一實施形態之電腦系統所進行之再生處理之順序圖。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 五、發明說明 ( 20 )

圖 5 係顯示在同一實施形態之電腦系統所進行之內容複製之順序圖。

### 主要元件對照表

1 0	網際網路
1 2	W E B 伺服器
1 1 1	應用程式
1 1 2	安全管理者
1 1 3	檔案系統
1 1 6	記錄媒體 A
1 1 7	記錄媒體 B

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

## 六、申請專利範圍

1. 一種電腦系統，係在記錄媒體可以記錄內容之電腦系統，其特徵為具備：

為了應記錄於前述記錄媒體之內容管理，記憶對應前述記憶媒體之 I D 之 I D 記憶手段（1 1 4 或 1 2 2），該 I D 記憶手段（1 1 4 或 1 2 2）係有別於前述記錄媒體而設置；

及在前述記錄媒體記錄內容之時，藉由前述 I D 記憶手段（1 1 4 或 1 2 2）使用對應前述記憶媒體之 I D，實施記錄前述內容之加密之內容管理手段（1 1 2）。

2. 如申請專利範圍第 1 項記載之電腦系統，其中上述 I D 記憶手段（1 1 4 或 1 2 2）之 I D 係藉由前述電腦系統之 B I O S 所管理，

前述內容管理手段（1 1 2）係藉由與前述 B I O S 之認證由前述 B I O S 取得前述 I D。

3. 如申請專利範圍第 2 項記載之電腦系統，其中前述 I D 記憶手段（1 1 4 或 1 2 2）係由儲存前述 B I O S 用之 B I O S - R O M 所構成，

前述 B I O S - R O M 具有使用者無法存取之安全領域，前述 I D 被儲存在該領域。

4. 一種電腦系統，其係可以在記錄媒體記憶內容之電腦系統，其特徵為包含：

記憶限制被附加在前述內容之再生／複製／移動用之控制資訊，以及對應前述記錄媒體之 I D 之記憶手段（

1 1 4 或 1 2 2），該記憶手段（1 1 4 或 1 2 2）係有

（請先閱讀背面之注意事項再填寫本頁）

訂

線



## 六、申請專利範圍

別於前述記錄媒體而設置；

及在被記錄於前述記錄媒體之內容的再生、或對其它記錄媒體之複製或移動被要求時，依據前述控制資訊與前述 I D，許可或禁止前述被要求之處理的實行之內容管理手段（1 1 2）。

5．如申請專利範圍第 4 項記載之電腦系統，其中前述內容管理手段（1 1 2）在將被記錄於不具有前述 I D 之記錄媒體（1 1 5）之內容移動於其它記錄媒體之情形，將被記錄於不具有前述 I D 之記錄媒體（1 1 5）之控制資訊以及內容移動於前述其它之記錄媒體後，消除被記錄在不具有前述 I D 之記錄媒體（1 1 5）之內容以及控制資訊。

6．如申請專利範圍第 5 項記載之電腦系統，其中前述內容管理手段（1 1 2）在對於被記錄於不具有前述 I D 之記錄媒體（1 1 5）之內容，被要求對其它之記錄媒體之複製、或對其它的記錄媒體之移動時，使用前述 I D 解除前述內容或其之密碼鍵之加密後，使用複製目的地或移動目的地之其它的記錄媒體之 I D，再度加密前述內容或其之內容的密碼鍵，記錄於前述其它之記錄媒體。

7．一種電腦系統，其特徵為包含：

記憶被使用於內容之安全管理用之裝置 I D（I D S）之裝置 I D 記憶手段（1 1 4 或 1 2 2）；

及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之裝置 I D，可以管理前述內容之加密／解碼之內容管

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

## 六、申請專利範圍

理手段（112），在不具有前述裝置ID之記錄媒體記錄內容之情形，使用前述裝置ID（IDS）管理前述內容之加密／解碼之內容管理手段。

8．如申請專利範圍第7項記載之電腦系統，其中上述裝置ID記憶手段（114或122）之裝置ID係藉由前述電腦系統之BIOS所管理，

前述內容管理手段（112）係藉由與前述BIOS之認證由前述BIOS取得前述裝置ID（IDS）。

9．如申請專利範圍第8項記載之電腦系統，其中前述裝置ID記憶手段（114或122）係由儲存前述BIOS用之BIOS-ROM所構成，

前述BIOS-ROM具有使用者無法存取之安全領域，前述裝置ID（IDS）被儲存在該領域。

10．如申請專利範圍第8項記載之電腦系統，其中在前述內容被附加限制該內容之再生／複製／移動用之限制資訊，

前述內容管理手段（112）在被要求被記錄於不具有前述媒體ID之記錄媒體（115）之內容之再生、對其它記錄媒體之複製、或對其它記錄媒體之移動時，依據前述控制資訊與前述改變檢測用編碼資料，許可或禁止前述被要求之處理的實行。

11．如申請專利範圍第10項記載之電腦系統，其中前述內容管理手段（112）在將被記錄於不具有前述ID之記錄媒體（115）之內容移動於其它記錄媒體之

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

## 六、申請專利範圍

情形，將被記錄於不具有前述 I D 之記錄媒體（1 1 5）之控制資訊以及內容移動於前述其它之記錄媒體後，消除被記錄在不具有前述 I D 之記錄媒體（1 1 5）之內容以及控制資訊。

1 2 . 如申請專利範圍第 1 1 項記載之電腦系統，其中前述內容管理手段（1 1 2）在對於被記錄於不具有前述媒體 I D 之記錄媒體（1 1 5）之內容，被要求對其它之記錄媒體之複製、或對其它的記錄媒體之移動時，使用前述裝置 I D（I D S）解除前述內容或其之密碼鍵之加密後，使用複製目的地或移動目的地之其它的記錄媒體之媒體 I D，再度加密前述內容或其之內容的密碼鍵，記錄於前述其它之記錄媒體。

1 3 . 一種電腦系統，其特徵為包含：

記憶被使用於內容之安全管理用之裝置 I D（I D S）之裝置 I D 記憶手段（1 1 4 或 1 2 2）；

及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之裝置 I D，可以管理前述內容之加密／解碼之內容管理手段（1 1 2），在不具有前述媒體 I D 之記錄媒體（1 1 5）記錄內容之情形，使用前述裝置 I D（I D S）管理前述內容之加密／解碼之內容管理手段（1 1 2）；

其中前述裝置 I D 記憶手段之裝置 I D 係藉由前述電腦系統之 B I O S 被管理，前述內容管理手段藉由與前述 B I O S 之認證由前述 B I O S 取得前述裝置 I D，在前述內容被附加限制該內容之再生／複製／移動用之限制資

（請先閱讀背面之注意事項再填寫本頁）

訂

線

## 六、申請專利範圍

訊，前述 B I O S 管理前述控制資訊之改變檢測用之編碼資料，前述內容管理手段在將被記錄於不具有前述媒體

I D 之內容複製於其它記錄媒體之情形，使前述內容之複製可能次數值減少 1 地更新不具有前述媒體 I D 之記錄媒體內之控制資訊，同時將被記錄於不具有前述媒體 I D 之記錄媒體之內容與前述更新後之控制資訊複製於前述其它之記錄媒體，而且依據更新後之控制資訊更新前述改變檢測用編碼資料之值。

1 4 . 如申請專利範圍第 1 3 項記載之電腦系統，其中前述內容管理手段（1 1 2）在對於被記錄於不具有前述媒體 I D 之記錄媒體（1 1 5）之內容，被要求對其它之記錄媒體之複製、或對其它的記錄媒體之移動時，使用前述裝置 I D（I D S）解除前述內容或其之密碼鍵之加密後，使用複製目的地或移動目的地之其它的記錄媒體之媒體 I D，再度加密前述內容或其之內容的密碼鍵，記錄於前述其它之記錄媒體。

1 5 . 一種電腦系統，係一種可以處理內容之電腦系統，其特徵為包含：

進行前述內容之安全管理之內容管理手段（1 1 2），該內容管理手段（1 1 2）包含：

在具有媒體 I D 之記錄媒體（1 1 6，1 1 7）記錄內容之情形，使用前述媒體 I D 加密前述內容或該內容之密碼鍵，記錄於具有前述媒體 I D 之記錄媒體之手段；

及在不具有媒體 I D 之記錄媒體（1 1 5）記錄內容

（請先閱讀背面之注意事項再填寫本頁）

訂 線

## 六、申請專利範圍

之情形，使用藉由前述電腦系統之 B I O S 被管理之前述電腦系統固有之裝置 I D ( I D S )，加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體 I D 之記錄媒體 ( 1 1 5 ) 之手段。

1 6 . 一種電腦系統，其特徵為具有：

電腦系統之硬體控制用之系統程式，該系統程式管理前述電腦系統固有之裝置 I D ( I D S )；

及利用前述電腦系統固有之裝置 I D ( I D S )，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼之內容管理手段 ( 1 1 2 )。

1 7 . 如申請專利範圍第 1 6 項記載之電腦系統，其中在前述內容被附加限制該內容之再生／複製／移動用之限制資訊，

前述系統程式管理前述控制資訊之改變檢測用之編碼資料，

前述內容管理手段 ( 1 1 2 ) 在被要求被記錄於前述媒體之內容之再生、對其它記錄媒體之複製、或對其它記錄媒體之移動時，依據前述控制資訊與前述改變檢測用編碼資料，許可或禁止前述被要求之處理的實行。

1 8 . 一種電腦系統，其係具有電腦系統所固有之裝置 I D ( I D S ) 之電腦系統，其特徵為包含：

由前述電腦系統取得前述裝置 I D ( I D S )，使用該取得之裝置 I D ( I D S ) 管理應記錄於前述電腦系統之記錄媒體之內容的加密／解碼之內容管理手段 ( 1 1 2

(請先閱讀背面之注意事項再填寫本頁)

訂 線

## 六、申請專利範圍

)。

19. 一種內容之保護方法，係提供一種被適用於可以處理內容之電腦系統，保護前述內容被不正當使用之內容保護方法，其特徵為：

在具有媒體 I D 之記錄媒體 ( 1 1 6 , 1 1 7 ) 記錄內容之情形，使用前述媒體 I D 加密前述內容或該內容之密碼鍵，記錄於具有前述媒體 I D 之記錄媒體 ( 1 1 6 , 1 1 7 ) ；

及在不具有媒體 I D 之記錄媒體 ( 1 1 5 ) 記錄內容之情形，使用藉由前述電腦系統內之 B I O S 被管理之前述電腦系統固有之裝置 I D ( I D S ) ，加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體 I D 之記錄媒體 ( 1 1 5 ) 。

20. 一種內容保護方法，其係一種保護以具有系統固有之裝置 I D ( I D S ) 之電腦系統被處理之內容被不正當使用之內容保護方法，其特徵為：

由前述電腦系統取得前述裝置 I D ( I D S ) ；

及使用前述取得之裝置 I D ( I D S ) ，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼。

21. 一種內容保護方法，其係一種保護在電腦系統被處理之內容被不正當使用之內容保護方法，其特徵為：

藉由前述電腦系統之硬體控制用之系統程式管理前述電腦系統固有之裝置 I D ( I D S ) ；

由前述系統程式取得前述裝置 I D ( I D S ) ；

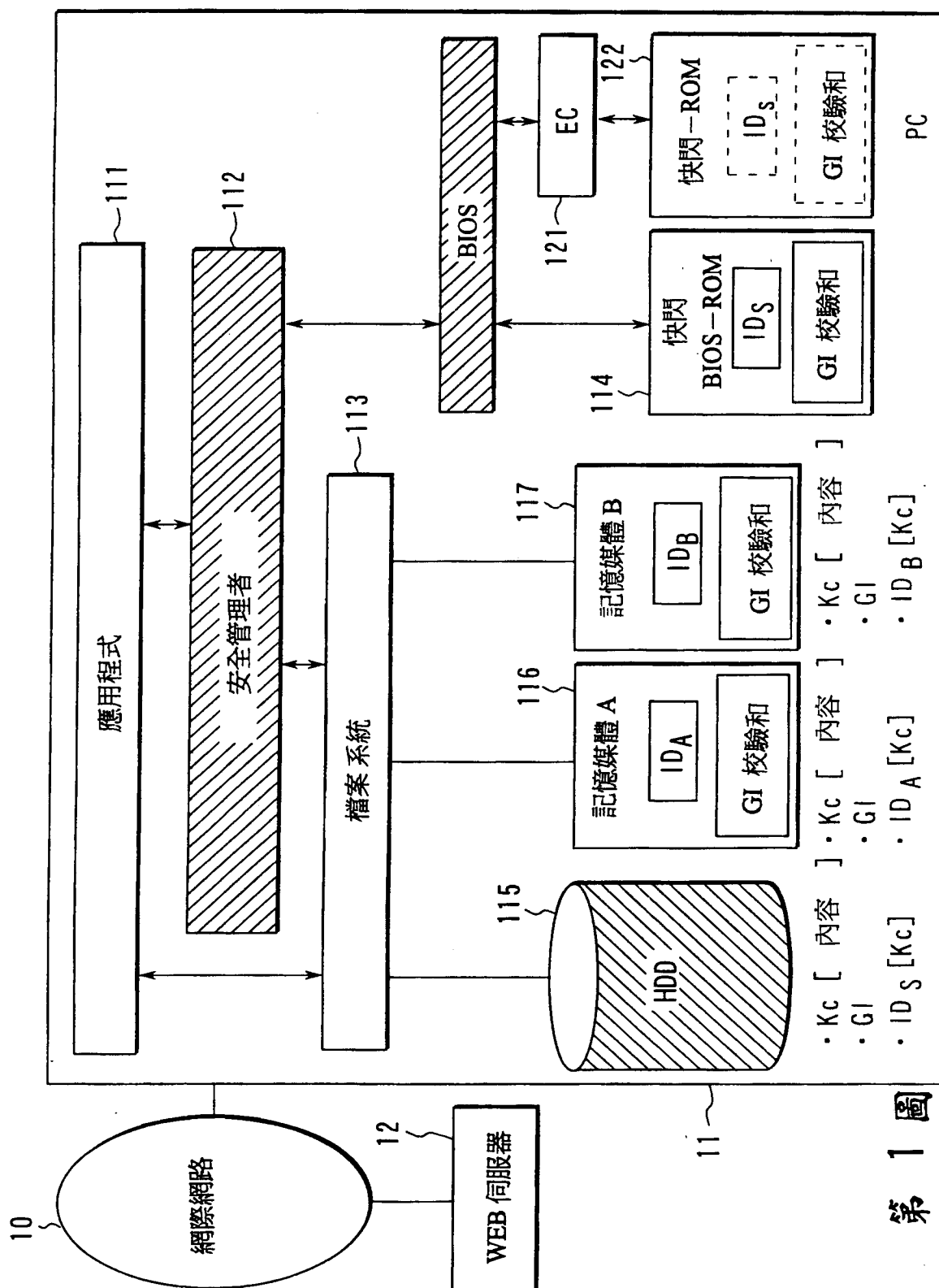
## 六、申請專利範圍

及使用前述取得之裝置 I D ( I D S ) , 管理應記錄於前述電腦系統之記錄媒體之內容之加密 / 解碼。

(請先閱讀背面之注意事項再填寫本頁)

訂

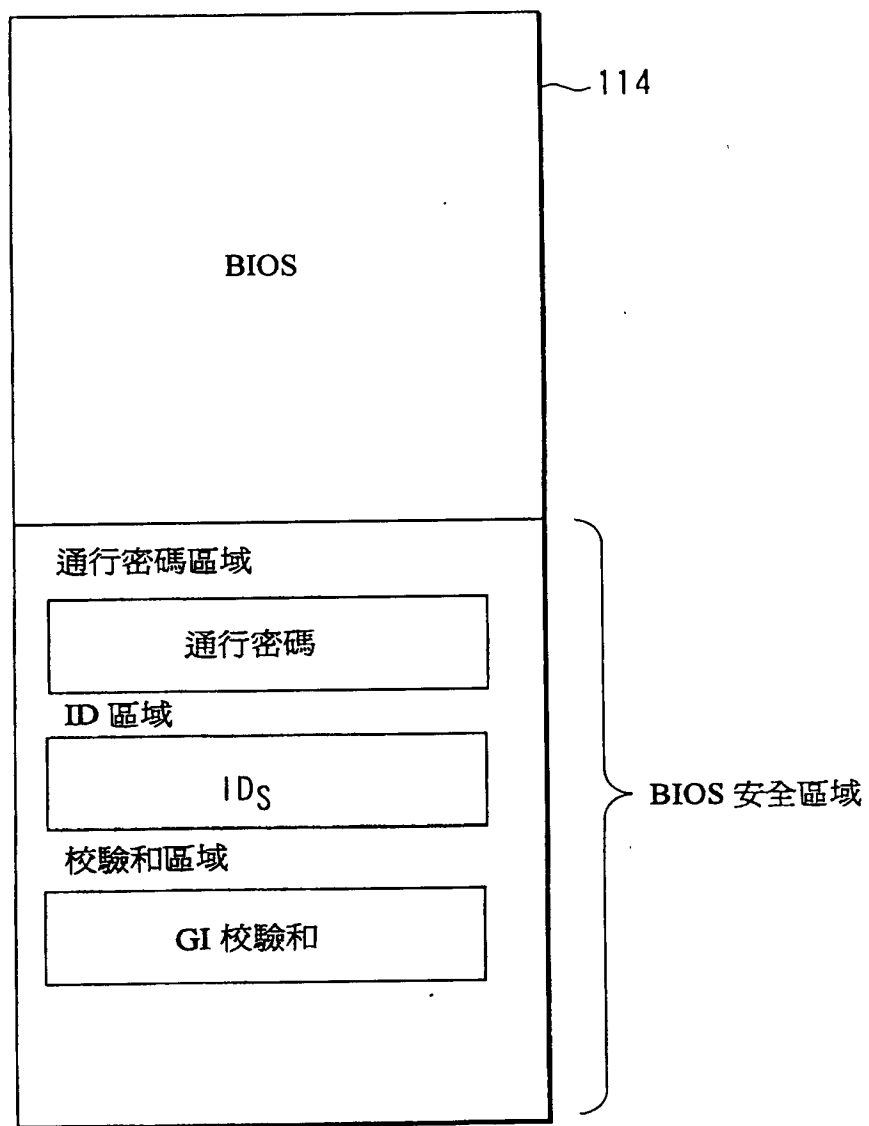
線



第 1 圖

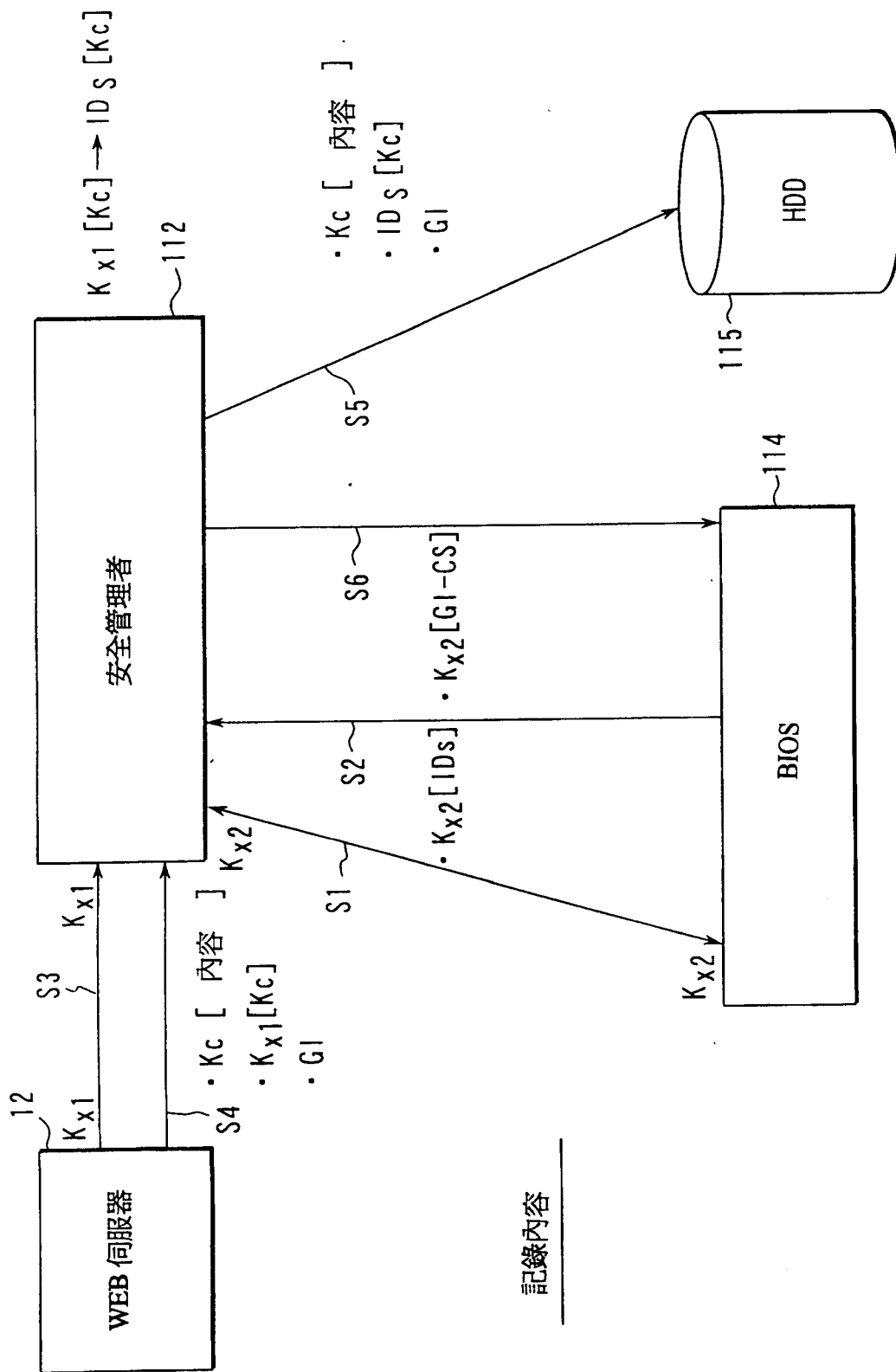


快閃 BIOS-ROM



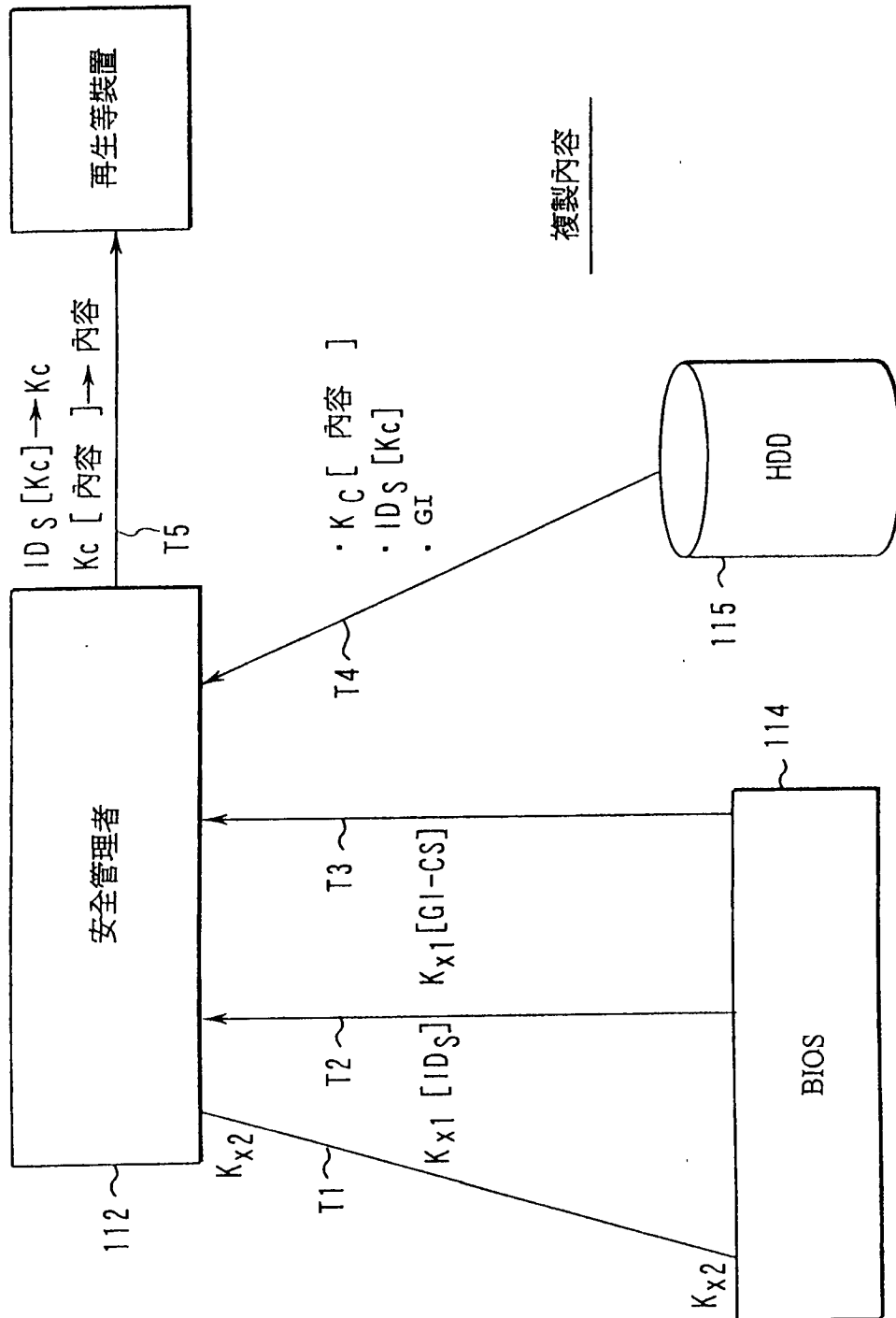
第 2 圖

89104427

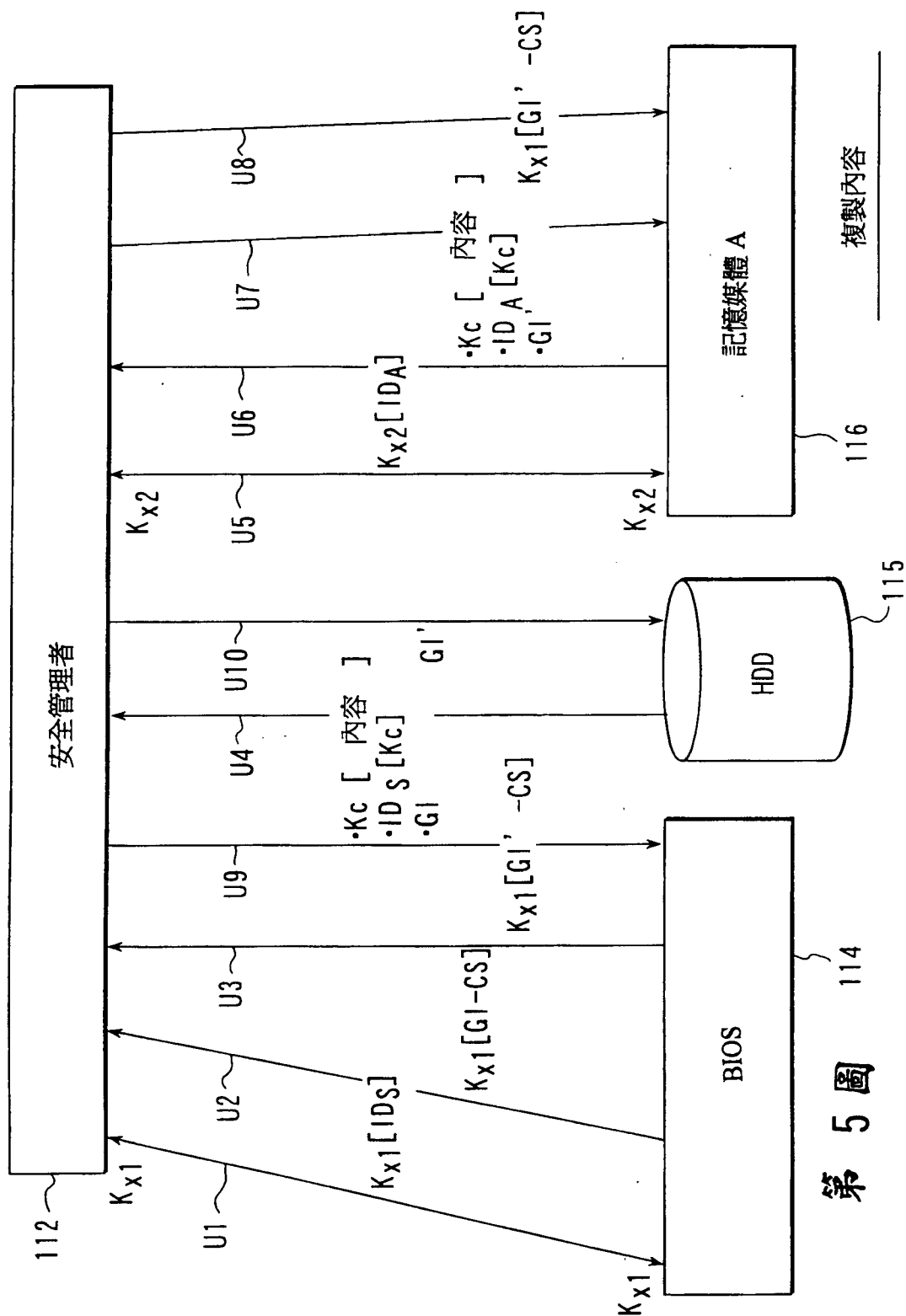


第 3 圖

90年11月2日 修正  
補充



第 4 圖



第 5 圖